IS your Business secure?

"Yes of course", I hear you say. We are emerging from recession, business is growing, new markets are emerging and we are making a profit. These are good times – bright future – what could go wrong?

However there is another consideration often overlooked by both small and large companies and that it is the vastly increasing risk of exposure to cyberattack and hackers gaining access to sensitive and customer's personal details. Imagine if the target was your company here in the Algarve!

The headlines in the world of cybercrime has recently been the cyberattack on UK's phone and broadband supplier TALKTALK, The personal details of up to 4 million customers may have been compromised, including credit card details and bank accounts. However, a week after the attack the company said it still did not know how much of their customer information had been encrypted.

Compounding this the company confirmed a week after the attack was disclosed that the number of people affected by the hack may be higher than previously thought, as this did not include millions of former customers whose details may still be held by the company .

It now appears that these sensitive personal details were not encrypted.

This is the latest in a number of high profile attacks against TALKTALK over the last 9 months, as well as other major companies.

A growing problem

According to Symantec's 2015 Internet Security Threat Report, **t**argeted cyberattacks against large companies increased by a whopping 40% in 2014 compared to the previous year. Even as the number of attacks surged, analysts found that the hackers were waging more efficient campaigns, deploying 14% less email to infiltrate an organization's network. It's not just big companies with various studies showing attacks against small companies with under 100 employees increasing at an alarming rate.

In addition to targeted attacks, non-targeted malware continues to proliferate online at a rate of **one million new threats a day**. Alarmingly corporate defences are falling behind as cybercriminals move faster.

As customers, we need ask the question on how vulnerable are major companies to cybersecurity attacks and whether they have systems in place to adequately protect our personal data.

This is probably a point which most people do not consider when choosing a service provider as we assume that our personal detail will be protected. However there are many experts who now believe that this should be one of the most important considerations given the scale of attacks that are now taking place.

Situation in the Algarve

There are many businesses operating here in the Algarve dealing with finance, currency exchange and banking plus solicitors and private companies who hold sensitive data regarding their customers. As cybercrime

respects no national and regional boundaries, all are potentially vulnerable, the same as would be elsewhere. In other words it is now the time to consider the advice given in this article by asking the question:

“Am I satisfied that I have adequate systems and processes in place to prevent hackers gaining access to sensitive information?”

Responsibility of companies

Business owners should now critically examine their systems especially those holding, sensitive customer information of their customers including bank account details, and data that is password protected.

In the sphere of corporate cyber warfare, phishing can provide hackers with a direct path into a company's network. Starting with nothing but an email address, they can make as many attempts as it takes to swipe the username and password that will allow them to access email accounts and virtual private network drives. Once this is accomplished, the attacker has enormous scope to grab data such as customers' personal information

All this makes it extremely important that companies protect themselves against phishing scams. Companies need to consider other security safeguards that limit how much damage a hacker can cause once a user account has been compromised. These could include the following:

- **Encryption for confidential documents and records**, so a hacker who gains access to the network proper is unable to get his or her hands on sensitive information without an additional key.
- **Non-use of email to send and receive high-risk data**, reducing the amount of information a hacker can access from a compromised email account. Instead, the company could use a secure messaging system with separate authentication for confidential documents and records.
- **A comprehensive audit trail to monitor network activity**, so that if a hacker succeeds in breaching the company's perimeter defences, this can be discovered and stopped as soon as possible.

Has your business implemented any of the above, or could you - and your intellectual property, and customers' personal information - be at risk of a phishing attack?

What can I do to protect my business?

Firstly by understanding the evolving risks.

Cybersecurity preparedness starts with having a complete understanding of the internal and external vulnerabilities that can affect any business, how hackers can gain entry including their different methods and motives, and how to identify points of weakness. Learn the different types of cyber fraud schemes and common threats – everything from phishing and spoofing scams, social engineering, malware, systems hacking, pharming, and everything in between.

Secondly, develop a security policy that is ingrained into corporate culture. Defining protocols to abide by is critical, but in order to be effective, the policy must permeate throughout every process, every decision, and the whole mentality of the organization – squarely embedded into its overall business strategy and how each employee operates. Educate your employees about the warning signs, safe practices, and responses to a suspected takeover. Make sure they use complex, unique passwords and maintain a “clean desk environment” where personal and confidential information aren’t exposed.

Thirdly pick up the phone. Verify financial requests and confirm details by phone instead of relying on email to initiate or complete any financial transaction – whether you are dealing with your bank, vendors, clients, or employees.

Use a two-step verification process to add another layer of security to approving outgoing funds – it will help protect you from a loss.

Fourthly keep your software up to date. Don't delay updating your anti-virus software or other security applications. Up to date software will help you guard against the latest threats and keep your infrastructure secure.

Have an incident response plan and practice it. Just like a fire drill, having a plan of action for responding to a cyber incident is crucial. Even more important, it should be practiced so that all your employees know exactly what to do in the event of a breach.

As cybercrime escalates and protection and preparedness become increasingly important for every organization both large and small, it's ultimately working together that will bolster the ability to combat mounting threats. In an environment where hackers are often one step ahead, a collective accountability can be our first line of defence.

We are pleased to help you

Safe Communities Algarve is pleased to run awareness sessions for local businesses in the Algarve on this topic to help you protect your systems. These will be conducted by Jim Litchko a computer security analyst who has written several books on this subject. Please contact info@safecommunitiesalgarve.com if your company is interested.

David Thomas

President

Safe Communities Portugal

Feature for Algarve Resident

26th November 2015